UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 07/11/2008

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) *1-25,34-41 and 43* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-33 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 08 April 2008. By this response, no claims have been amended, added, or canceled. Claims 1-25, 34-41, and 43 were previously withdrawn from further consideration as being drawn to nonelected inventions. Claims 26-33 and 42 are currently under consideration in the present application.

Response to Arguments

2. Applicant's arguments filed 08 April 2008 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 26-33 and 42 under 35 U.S.C. 103(a) as unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in view of Vanstone et al, US Patent 6337909, Applicant argues that the cited prior art does not teach the steps recited in independent Claim 26.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, Applicant argues that Kocher does not teach the step of previously determining and storing the auxiliary function (see, for example, page 2 of the present response). However, Kocher was not relied upon to teach this step; rather, the

Vanstone reference was relied upon to show this limitation. Further, Applicant argues that Vanstone does not disclose input data falsification with auxiliary data or compensating for the falsification with an auxiliary function value (page 2 of the present response). However, Vanstone was not relied upon to teach those steps; rather, Kocher was relied upon to show those limitations, and Applicant clearly acknowledges that Kocher does show those limitations (see pages 2 and 5 of the present response). The Examiner submits that the combination of the steps disclosed by Kocher (see paragraphs 0068, 0070, 0072, and 0073, as previously cited) with the general teaching in Vanstone of pre-computation of secret values (see column 3, lines 16-21; column 4, lines 1-5 and 42-44; column 2, lines 20-22, as previously cited; see also, for example, claim 2, at column 7, lines 17-18) therefore renders the claimed invention unpatentable.

Applicant further argues that, although Vanstone generally discusses pre-computing values, Vanstone does not relate to an "auxiliary function value" as claimed (pages 2-3 of the present response), and that Applicant "is not claiming the general principle of pre-computing secret values in a secure environment" (pages 3-4 of the present response). In response, the Examiner notes that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference; nor is it that the claimed invention must be expressly suggested in any one or all of the references. Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981). Specifically, the Examiner submits that the broad teaching within Vanstone of pre-computing and storing

secret values securely (see column 3, lines 16-21; column 4, lines 1-5 and 42-44; column 2, lines 20-22, as previously cited; see also, for example, claim 2, at column 7, lines 17-18) would have suggested to one of ordinary skill in the art at the time the invention was made to modify the method already disclosed by Kocher to include that pre-computation of the secret values.

In response to Applicant's argument that Vanstone is nonanalogous art, or more specifically, that Vanstone "concerns a very different problem" (page 3 of the present response), it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Vanstone is at least reasonably pertinent to the particular problem with which applicant is concerned, namely, the prevention of disclosure of secret values used in encryption or other secure calculations (see Vanstone, generally discussing secret keys, column 1, lines 15-58; see also column 2, lines 7-22, and column 3, lines 19-21, where the secret value is maintained securely).

Further, Applicant argues that Vanstone uses the term "secure" in a different sense than that of the present invention; Applicant asserts that Vanstone uses the term in the sense of "computationally secure" and that Vanstone discloses no measures "to prevent an attacker from spying out the secret key k by monitoring the computation k = k' + i that is used to store i securely" (see page 4 of the present response). First, the Examiner notes that, while Vanstone does use the phrase "computationally secure" (for

example, at column 2, lines 19), Vanstone also appears to use the term "secure" in the more general sense, as in the phrase "maintained securely" at column 3, line 21, where, since the values that are stored and "maintained securely" are secret, Vanstone at least suggests that at least some protection of those values is undertaken. More tellingly, Vanstone also explicitly refers to values being "maintained secret" (see column 7, lines 17-18, in claim 2). Clearly, some precaution is taken, or at the very least contemplated, to keep the values secret and secure, although Vanstone may not explicitly disclose what specific actions are taken. Additionally, the Examiner notes that Applicant's assertion as quoted above ("No measures are… disclosed by Vanstone to prevent…", page 4 of the present response) is generally unclear. First, Applicant does not provide any citations as to which portion of Vanstone is being referenced by the equality "k = k' + i", and it is not clear as to where this appears in Vanstone. Second, there appears to be an inconsistency as to which value in Vanstone Applicant is suggesting would need to be protected by measures such as those disclosed in the present specification or in Kocher; Applicant previously asserted that the value γ would be the value that is pre-computed and stored (see pages 2-3 of the present response), but Applicant also refers to "spying out the secret key k", storing the value i securely, and protecting k or k' (page 4 of the present response).

In response to Applicant's argument that there is no suggestion to combine the references (page 4 of the present response), the Examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation

to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Applicant has first argued that one of the previously cited motivations to combine the references, namely the pre-storing of values to achieve faster computation (Vanstone, column 3, lines 22-27, as previously cited), does not appear to be applicable to the method of Kocher (page 4 of the present response). However, the Examiner respectfully disagrees. The Examiner notes that, even if there were not significant overall gains in computation speed or overhead from pre-computing and storing the values used in Kocher, such as those cited by Applicant, there still would be an advantage gained by pre-computing and storing various values as taught by Vanstone, because the steps required to generate the auxiliary function value would be performed prior to the processing required to perform the remaining steps, and would thus reduce overhead during those steps. More specifically, if the claimed auxiliary function value (as taught by Kocher) were previously calculated and stored (as taught by Vanstone), then the fact that the auxiliary value would need only be loaded, rather than calculated, as required, would shift some of the computational overhead to a preliminary step of the pre-computation rather than adding to the overhead required during the main steps of "falsifying" and "combining" (i.e. compensating) as claimed. Therefore, the Examiner submits that the previously cited reasoning of allowing faster computation, as taught by Vanstone, would still have provided motivation to combine the Kocher and Vanstone references. Parenthetically, the Examiner notes that

Applicant's mention of loading values "from a disc" (see page 4 of the present response) does not appear to have any support in Vanstone, Kocher, or the present specification; there is nothing in either of those references or Applicant's own disclosure to suggest that a separate disk would be used for storage of these values, especially given that at least the Kocher reference is primarily directed to smart cards or other tamper resistant devices (see Kocher, abstract). Further, even assuming *arguendo* that allowing faster computation, as taught by Vanstone, would not have been sufficient motivation to combine the references, the Examiner submits that additional motivation would have been provided to combine the teachings of Vanstone with the method of Kocher in order to allow maintenance of security (Vanstone, column 3, lines 16-27; see also column 2, lines 20-22, as previously cited).

Therefore, for the reasons detailed above, the Examiner maintains the rejection as set forth below.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 26-33 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al, US Patent Application Publication 2002/0124178, in view of Vanstone et al, US Patent 6337909.

In reference to Claim 26, Kocher discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data before execution of one or more operations (paragraphs 0068, 0070, and 0072, where blinding occurs before permutation operations), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data (paragraphs paragraphs 0070, 0072, and 0073, where unblinding occurs to compensate for the blinding), where the auxiliary value was determined by executing the operations using the auxiliary data as input data (paragraph 0072, where the output buffer is initialized with the blinding bit and the data in the output buffer is the result of using the input permutation table, i.e. the operations). However, while Kocher discloses previously determining the auxiliary data and/or values (see paragraph 0072), Kocher does not explicitly disclose determining the auxiliary value previously and in safe surroundings.

Vanstone discloses a method in which secret values are precomputed in safe surroundings and where the secret values are maintained securely (see, for example, column 3, lines 16-21; column 4, lines 1-5 and 42-44; see also column 2, lines 20-22) in order to allow faster computations (see column 3, lines 22-27, for example). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kocher to include precomputation and safe storage

of secret values in order to allow faster computations and maintenance of security (see Vanstone, column 3, lines 16-27; see also column 2, lines 20-22).

In reference to Claim 27, Kocher and Vanstone further disclose that the combination with the auxiliary function value is performed before execution of a non-linear operation (see Kocher, paragraph 0074, where inputs can be maintained in a blinded state and only reconstituted when nonlinear operations must be performed).

In reference to Claim 28, Kocher and Vanstone further disclose that the auxiliary data are varied (Kocher, paragraphs 0072-0075; Vanstone, column 3, lines 8-27).

In reference to Claims 29-32, Kocher and Vanstone further disclose that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (see Kocher, paragraphs 0072 and 0075; Vanstone, column 3, lines 16-21; column 4, lines 1-5).

In reference to Claim 33, Kocher and Vanstone further disclose combining the output data and auxiliary function value using an XOR operation (see Kocher, paragraph 0073).

In reference to Claim 42, Kocher and Vanstone further disclose that operations include permutations of data (see Kocher, paragraphs 0068 and 0070-0074).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Vanstone et al, US Patent 7372961, discloses a system in which a number is masked by combination with a precomputed value. It is noted that this reference does not constitute prior art to the present application, but is included for the sake of completeness.

b. Kocher et al, US Patent Application Publication 2008/0104400, discloses a system in which various random numbers and secret values are precomputed.

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137